INTERNATIONAL SCIENTIFIC CONFERENCE
20-22 November 2025, GABROVO

REVIEW OF QUANTITATIVE METHODS FOR ASSESSING RESILIENCE IN COMPUTER NETWORKS

Erkan Salimov Yakubov [1], Plamen Stanchev [2]

[1]Technical University of Sofia, Department of Cybersecurity, 8, Kliment Ohridsky blvd. Sofia, Bulgaria
[2]Technical University of Sofia, Department of Computer Systems, 8, Kliment Ohridsky blvd. Sofia, Bulgaria

Abstract
The paper presents a review of quantitative methods for assessing resilience in computer networks. The concept of network resilience is analyzed in terms of its relationship to reliability, robustness, and fault tolerance. Various groups of methods are discussed, including probabilistic, graph-based, and simulation approaches, as well as modern artificial intelligence models for resilience evaluation. Comparative analysis highlights the advantages and limitations of each class of methods and their applicability to different network architectures. The aim of the study is to provide a structured overview and framework for selecting an appropriate quantitative evaluation method depending on network topology, performance requirements, and external risk factors.
Keywords: resilience, reliability, computer networks, quantitative assessment, fault tolerance, artificial intelligence.

INTRODUCTION

With the increasing dependence of society and industry on computer and communication networks, assessing their resilience is gaining strategic importance. Resilience describes the ability of a system to maintain functionality in the presence of failures, overloads or malicious attacks.

In the modern digital era, characterized by the integration of critical infrastructures, cloud services and distributed computing environments, resilience is becoming a multidisciplinary concept. It encompasses not only the technical aspects of reliability and fault tolerance, but also organizational measures related to cybersecurity, service continuity and risk management [1-3].

With the advent of 5G, IoT and Edge technologies, network architectures are becoming more decentralized, which increases the number of potential points of failure. Traditional approaches to reliability analysis often prove insufficient, as they do not take into account the dynamics of loads, self-organizing protocols and the interconnections between communication and physical components [4, 5].

The need for quantitative methods for assessing resilience stems from the need for an objective comparison of different topologies, architectures and incident response strategies. In this context, simulation and artificial intelligence approaches that enable real-time prediction, adaptability and self-healing of systems are gaining increasing importance.

Distributed energy resources (DER) and integrated renewable energy systems introduce new challenges to the resilience of communication and energy networks. The hybrid nature of these systems, a combination of physical (energy) and digital (communication) infrastructure, increases vulnerability to both technical and cyber threats [6].

doi: www.doi.org/10.70456/.....

The main risks can be grouped into three categories: Physical failures: overload, inverter failure, interruption of connections between nodes; Cyber threats: DDoS attacks, unauthorized access to controllers, manipulation of sensor data; System violations: cascading failures due to unsynchronized operations between network components [7].

Resilience in such environments must take into account both the ability to automatically restore functionality and the dynamic response capacity of intelligent controllers. Therefore, hybrid resilience models are applied in modern microgrids, including AI algorithms for anomaly detection, predictive diagnostics and adaptive load management [8].

Architectural approaches to building resilient infrastructure are focused on zoning, modularity and access control. By dividing the network into independent zones with limited communication links between them, the risk of avalanche-like propagation of failures or attacks is reduced.

Modern concepts such as Defense-in-Depth and Zero Trust Architecture are fundamental to achieving cyber resilience. They require multi-layered protection, where each component is treated as a potential source of risk, and access is dynamically controlled based on context and behavior.

Graph models are particularly useful in analyzing zonal resilience by calculating algebraic connectivity (λ_2), edge betweenness, and node centrality, which can assess the ability of a network to remain connected in the event of node or link loss. These metrics help identify critical points, optimize redundancy, and assess the effectiveness of zoning policies.

Quantitative assessment of cyber resilience requires clearly defined metrics to measure the responsiveness and adaptability of the system. Among the main Key Performance Indicators (KPIs) are presented in Table 1.

Table 1 Main Key Performance Indicators (KPIs)

Indicator	Description	Unit
Mean Time to Detect (MTTD)	Average time to detect an incident	s/min
Mean Time to Repair (MTTR)	Average time to respond and recover	s/min
Resilience Index (RI)	Ratio between availability before and after failure	–
Cyber Impact Factor (CIF)	Measure of the impact of a cyber incident on performance	%
Service Availability Ratio (SAR)	Proportion of time the service is available	%

Combining these metrics provides a comprehensive view of the technical and management aspects of resilience. For example, a high SAR value combined with a low MTTR means that the network can recover its functionality quickly even in the event of complex disturbances. These KPIs can be integrated into automated monitoring systems driven by artificial intelligence that can maintain dynamic resilience dashboards in real time.

The resilience of computer and cyber-physical networks is becoming a key indicator of security and efficiency in the digitalized economy. The synergy between classical quantitative methods and modern AI approaches opens up new opportunities for real-time adaptation, failure prediction and self-healing of systems.

Future research should focus on integrating resilience indices into microgrid and cyber-physical infrastructure management systems, as well as on developing standardized methodologies for measuring cyber resilience. This will enable the achievement of reliable, intelligent and energy-efficient networks, ready to adapt to the dynamic environment of modern digital ecosystems.

Resilience is the ability of a network system to maintain an acceptable level of

doi: www.doi.org/10.70456/.....

functionality in the presence of disturbances, damage, or malicious impacts and to restore normal operation in a short time. It builds on the traditional concepts of reliability, recoverability, and fault tolerance, adding aspects of adaptability and self-organization. From a theoretical point of view, resilience can be viewed as a function of three main components: Performance robustness, the ability of the system to maintain key services even under disturbed conditions; Adaptability – the ability to change the topology, routing, or control strategy in response to deviations; Recoverability – the speed and efficiency of the recovery process after an incident.

Classical reliability models use a probability function *R(t)*, defined as the probability that the network will be operational at time t:

$$R(t) = P(\text{Network operational at time } t) \quad (1)$$

The average failure and recovery rates are expressed by Mean Time Between Failures (MTBF), Mean Time to Repair (MTTR). System availability is defined as:

$$A = \frac{MTBF}{MTBF + MTTR} \quad (2)$$

These dependencies form the basis for quantitative assessment of resilience, but in dynamic networks (5G, IoT, SDN, Cloud) they need to be extended with temporal and behavioral factors.

Modern approaches treat resilience as a dynamic metric *Res(t)*, which depends on the current state of the network, the recovery rate, and its adaptive response:

$$R_{es}(t) = f[R(t), A(t), R_{es}(t), A_{dapt}(t)] \quad (3)$$

where:

•*R(t)* – probability that the network is functional;

•*A(t)* – instantaneous availability;

•*Rec(t)* – recovery index;

•*Adapt(t)* – adaptability to changing conditions.

This achieves a holistic view of the system's behavior in complex scenarios, from physical damage to cyberattacks.

In the context of cyber-physical systems (e.g. smart energy grids, industrial IoT), resilience includes not only hardware and software failures, but also the ability to respond to cyberattacks and data anomalies. Cyber resilience adds to the classic definition elements such as incident detection (Detection), response and mitigation (Response & Mitigation), and adaptation of access and routing policies. In this sense, a resilient network does not simply recover after a failure, but evolves, using the accumulated experience to improve the response to future events.

For practical assessment of resilience, integral indicators combining accessibility, recovery time, and functional degradation are used. One of the most commonly applied is the Resilience Index (RI):

$$RI = \frac{A_{post}}{A_{pre}} \cdot \frac{T_{rec}}{T_{tot}} \quad (4)$$

where:

- *Apre* – availability before failure;
- *Apost* – availability after failure;
- *Trec* – recovery time;
- *Ttot* – total observation period.

The higher the value of RI, the less functional degradation and the better the resilience of the system.

In cyber-physical environments, this metric is often combined with Cyber Impact Factor (CIF) and Service Availability Ratio (SAR) to account for the impact of cyber incidents on overall performance.

MAIN METHODS FOR QUANTITATIVE ASSESSMENT

- Probabilistic methods

They model failures as a stochastic process. Probability distributions are used: exponential, Weibull, and Poisson. The goal is to calculate the probability that the network will remain functional with a

doi: www.doi.org/10.70456/.....

certain number of failures. The method applies to large but stable infrastructures with known failure statistics.

- Graph methods

Quantitative assessment of resilience in computer networks aims to objectively measure their ability to function and recover from disturbances. The main methods can be grouped into four categories:

- Probabilistic methods

They model failures as stochastic processes using distributions such as exponential, Weibull, and Poisson. They allow calculating the probability that the network will remain functional with a given failure intensity. They are suitable for stable infrastructures with known failure statistics and are used to calculate MTBF, MTTR, and availability A.

- Graph methods

The network is represented as a graph G(V,E), in which nodes and links reflect real elements. Metrics such as node connectivity, edge connectivity, and algebraic connectivity (λ_2) allow for the assessment of topological resilience and the identification of critical points. These methods are effective in the analysis of complex or large-scale infrastructures, including 5G and IoT environments.

- Simulation methods

They are used to analyze the dynamic behavior under various failure scenarios. Monte Carlo and agent-based simulations (via OMNeT++, NS-3, NetworkX) allow for the tracking of the time evolution of the network and the estimation of the Resilience Index (RI) in realistic conditions. This approach is flexible, but requires high computing power.

- Methods based on artificial intelligence

AI approaches introduce adaptability and predictive capabilities: Neural networks (ANN, LSTM) – failure and load prediction; Fuzzy Logic – estimation under uncertainty; Reinforcement Learning (RL) – self-learning incident response management. In modern systems, these methods are often integrated into Digital Twins, which provide real-time assessment and optimization of resilience.

COMPARATIVE ANALYSIS OF METHODS

The comparison between the different approaches for quantitative resilience assessment shows that each method has specific advantages and limitations. Probabilistic models offer high analytical accuracy when reliable failure statistics are available, but are not applicable to dynamic or self-organizing topologies. Graph methods provide a clear structural model and allow visualization of critical nodes and connections in the network, but do not take into account the time evolution and changes in load. Simulation approaches are distinguished by high realism and the ability to analyze different failure scenarios, the main disadvantage of which is the need for significant computational resources. Methods based on artificial intelligence offer the greatest adaptability and prognostic potential, as they can be trained on historical data and assess resilience in real time, but require preliminary preparation of large data sets.

Hybrid solutions combining probabilistic, graph, and AI analysis demonstrate an optimal balance between accuracy, flexibility, and scalability. The integration of these approaches into digital twins and predictive control platforms enables continuous monitoring, automated diagnostics, and self-learning improvement of the resilience of network systems.

MAIN TRENDS

Modern research in the field of resilience of computer and cyber-physical networks is directed towards the integration of intelligent and hybrid approaches. There is a trend towards combining graph and probabilistic models in multilayer architectures, which more accurately describe the relationships between physical and logical components. Big Data Analytics methods are increasingly being applied,

doi: www.doi.org/10.70456/.....

allowing for the discovery of patterns and the prediction of incidents based on real loads and historical events.

Significant progress is being achieved by integrating artificial intelligence for automated diagnostics, predictive maintenance, and self-tuning of network parameters. The development of concepts such as digital twins and reinforcement learning controllers supports the simulation and optimization of resilience in real time. In parallel, the scope of assessment is being expanded by including indicators of energy resilience and cyber resilience, especially in decentralized systems such as IoT and DER networks.

These trends outline a transition from static to adaptive models, in which sustainability is viewed as a continuous process of monitoring, learning, and optimization.

CONCLUSION

Quantitative assessment of resilience in computer and cyber-physical networks is evolving from static engineering-probabilistic analysis to intelligent, adaptive, and hybrid models. Classical methods provide a basis for structural and statistical assessment, but do not reflect the dynamics and complexity of modern networks. The integration of artificial intelligence, big data, and simulation techniques allows the construction of self-monitoring and self-learning systems, capable of responding and recovering in real time. Future research should be directed towards standardizing cyber resilience metrics, implementing digital twins, and developing autonomous controllers based on reinforcement learning. These approaches will allow the construction of networks with high adaptability, predictability, and resilience, which can guarantee continuity and security in the conditions of increasing connectivity and cyber dependence.

Funding: The studies were conducted under project BG-RRP-2.004-0005 "Improving the research capacity and quality to achieve international recognition and resilience of TU-Sofia (IDEAS)".

Acknowledgments: The studies were conducted under project BG-RRP-2.004-0005 "Improving the research capacity and quality to achieve international recognition and resilience of TU-Sofia (IDEAS)".

REFERENCE

[1] J. P. G. Sterbenz et al., “Resilience and survivability in communication networks: Strategies, principles, and survey of disciplines,” Computer Networks, vol. 54, no. 8, pp. 1245–1265, Mar. 2010, doi: 10.1016/j.comnet.2010.03.005..

[2] M. Oehlers and B. Fabian, “Graph Metrics for Network Robustness—A survey,” Mathematics, vol. 9, no. 8, p. 895, Apr. 2021, doi: 10.3390/math9080895.

[3] T. Vatten, "Investigating 5G Network Slicing Resilience through Survivability Modeling," 2023 IEEE 9th International Conference on Network Softwarization (NetSoft), Madrid, Spain, 2023, pp. 370-373, doi: 10.1109/NetSoft57336.2023.10175399.

[4] M. Awad, F. Sallabi, K. Shuaib, and F. Naeem, “Artificial intelligence-based fault prediction framework for WBAN,” Journal of King Saud University - Computer and Information Sciences, vol. 34, no. 9, pp. 7126–7137, Sep. 2021, doi: 10.1016/j.jksuci.2021.09.017.

[5] D. Dwivedi, K. V. S. M. Babu, P. K. Yemula, P. Chakraborty, and M. Pal, “A comprehensive metric for resilience evaluation in electrical distribution systems under extreme conditions,” Applied Energy, vol. 380, p. 125001, Dec. 2024, doi: 10.1016/j.apenergy.2024.125001.

[6] Digital Europe Programme,” European Commission. https://commission.europa.eu/funding-tenders/find-funding/eu-funding-programmes/digital-europe-programme_en

[7] L. Wang, X. Weidong, and L. Xiaoxia, “Intelligent monitoring and control of power systems based on artificial intelligence technology,” Procedia Computer Science, vol. 247, pp. 963–969, Jan. 2024, doi: 10.1016/j.procs.2024.10.116.

[8] C. Pak, “Responsible AI and algorithm governance: An institutional perspective,” in Elsevier eBooks, 2022, pp. 251–270. doi: 10.1016/b978-0-323-85648-5.00018-9.

doi: www.doi.org/10.70456/.....